<center>REMARKS</center>

Claims 1-7 and 17-20 are pending in the present application. Applicants respectfully request reconsideration of the present application in view of the remarks presented herein.

<center>35 U.S.C. § 103</center>

Claims 1, 3-5, 7, 17, 18 and 20 stand rejected as allegedly unpatentable over Spies et al. (US 6,055,314, "Spies") in view of Deo et al. (US 5,721,781, "Deo"). Applicants have carefully reviewed the cited references and respectfully assert that embodiments of the present invention as recited in Claims 1, 3-5, 7, 17, 18 and 20 are patentable over Spies in view of Deo.

The rejection proposes to modify Spies in view of Deo. However, Doe teaches an authentication system that is dependent upon hardware comprising global secrets, e.g., digital certificates (Abstract). However, Spies specifically teaches away from such a system. "It is therefore another object of this invention to provide a ... system that has no global secrets built into any hardware..." (Spies, column 2 lines 1-5). Consequently, Applicants respectfully assert that one of ordinary skill in the art would be taught away from the proposed modification of Spies in view of Deo in view of the teachings of Spies.

For this reason, Applicants respectfully assert that Claims 1, 3-5, 7, 17, 18 and 20, and all other claims rejected over a combination of Spies with Deo, overcome the rejections of record, and respectfully solicit allowance of these Claims.

With respect to Claim 1, Applicants respectfully assert that Spies in view of Deo fails to teach or fairly suggest the limitation "at said first logical circuit, decrypting said encrypted signal using said first decryption key" as recited by Claim 1.

In contrast, Spies teaches, "[t]he view computing unit 60 is not permitted, however, to read the decryption capabilities" (column 9, lines25-26, emphasis added) and "the individual packet keys are never made available to the viewer computing unit..." (column 10, lines 46-47, emphasis added). Thus, in accordance with the teaching of Spies, the recited "first logical unit" does not decrypt the accessed encrypted signal, and further does not decrypt the accessed encrypted signal using the recited "first decryption key."

In teaching benefits of keeping decryption capabilities and packet keys solely within the IC card, Spies actually teaches away from embodiments of the present invention that recite transferring a decryption key to a decoding unit.

While the proposed modification of Spies in view of Doe is alleged to teach encryption and decryption of the recited first decryption key, Applicants respectfully assert that such teaching, even if present, does not remedy this deficiency of Spies, nor does the rejection allege that it does.

For these reasons, Applicants respectfully assert that Claim 1 overcomes the rejections of record, and respectfully solicit allowance of this Claim.

The rejection argues, "the CPU of the set top box (first logical unit) receives the decryption key from the IC card to decrypt the encrypted signal." Applicants respectfully assert that such a teaching fails to teach or suggest embodiments of the present claimed invention as recited in Claim 1.

Claim 1 recites, in part, the following limitations:

d) encrypting said first decryption key at said second logical circuit by use of said public encryption key;

e) transferring said encrypted first decryption key from said second logical circuit to said first logical circuit over a communication link;

f) at said first logical circuit, decrypting said encrypted first decryption key by use of a secret key to determine said first decryption key

Applicants respectfully assert that Spies fails to teach or fairly suggest the recited limitations of encrypting a decryption key, transferring the encrypted

encryption key to another logical unit, and decrypting the encrypted decryption key.

Deo fails to remedy this deficiency of Spies as Deo fails to teach or fairly suggest use of the digital certificate exchange technique for uses other than certificate exchange.

For this additional reason, Applicants respectfully assert that Claim 1 overcomes the rejections of record, and respectfully solicit allowance of this Claim.

Applicants respectfully assert that Claims 2-7 overcome the rejections of record by virtue of their dependency, and respectfully solicit allowance of these Claims.

In addition with respect to Claim 4, Applicants respectfully assert that Spies in view of Deo fails to teach or fairly suggest the limitation "replacing a computer control program stored in a second portion of local memory at said second logical circuit with a new computer control program" in conjunction with the other limitations as recited by Claim 4.

While Spies may teach that CSPs can be changed or updated, Spies does not teach a method or system for such updates. In particular, Spies teaches such CSPs are "preferably ... stored in ROM (read only memory)" (column 11 lines 64-66). Applicants respectfully assert that one of ordinary skill in the art would understand that changing software stored in a ROM requires physical replacement of the ROM device. Moreover, software "stored in ROM" cannot be replaced as recited by Claim 4, as a ROM is, by definition, not writable. Consequently, Spies fails to teach updating software within the operation of the media system, as recited by Claim 4.

Deo is not alleged to correct this deficiency of Spies, and Applicants respectfully assert that it does not.

For these additional reasons, Applicants respectfully assert that Claim 4 overcomes the rejections of record, and respectfully solicit allowance of this Claim.

In addition with respect to Claim 7, Applicants respectfully assert that Spies in view of Deo fails to teach or fairly suggest the limitation "wherein said digital signal is substantially compliant with the Motion Pictures Experts Group (MPEG) format" as recited by Claim 7.

While Spies may teach the "video content can be TV broadcasts" as stated in the rejection, Applicants respectfully assert that the recited signal is not limited to "TV broadcasts" or even to video. For example, it is well known that compact disc (CD) audio is digital; however, it is generally not encoded in MPEG.

Moreover, the cited references do not teach or fairly suggest MPEG compliant signals. Both references are completely silent as to MPEG. The Examiner is invited to introduce art that teaches MPEG or to withdraw the rejection.

The Advisory Action states that "the MPEG-2 video format is the video format used for satellite television and DVDs." However, no art is introduced to support this statement. Applicants respectfully note that MPEG-2 video is not used for all satellite television. For example, MPEG-2 is not used for analog satellite television transmission. The Examiner is respectfully requested to introduce art that teaches MPEG or to withdraw the rejection.

For these additional reasons, Applicants respectfully assert that Claim 7 overcomes the rejections of record, and respectfully solicit allowance of this Claim.

With respect to Claim 17, Applicants respectfully assert that Claim 17 overcomes the rejections of record for at least the rationale previously presented with respect to Claim 1, and respectfully solicit allowance of this Claim.

Applicants respectfully assert that Claims 18-20 overcome the rejections of record by virtue of their dependency, and respectfully solicit allowance of these Claims.

In addition with respect to Claim 19, Applicants respectfully assert that Claim 19 overcomes the rejections of record for at least the rationale previously presented with respect to Claim 4, and respectfully solicit allowance of this Claim.

In addition with respect to Claim 20, Applicants respectfully assert that Spies in view of Deo fails to teach or fairly suggest the limitation, "(a system) configured such that the contents of said local memory cannot be observed from outside of said first logical circuit," as recited by Claim 20.

In fact, Spies directly <u>teaches</u> <u>away</u> from this recited limitation, teaching that the CPU (a second logical unit) accesses the dynamic linked libraries (software) stored on the IC Card (first logical unit). By such teaching, Spies clearly teaches that the contents of the first logical unit are not only observable,

but necessarily utilized by other logical units, in direct contrast to the recited limitation.

For this additional reason, Applicants respectfully assert that Claim 20 overcomes the rejections of record, and respectfully solicit allowance of this Claim.

Claim 2 stands rejected as allegedly unpatentable over Spies et al. (US 6,055,314, "Spies") in view of Deo et al. (US 5,721,781, "Deo") and further in view of Schneier (Applied Cryptography, 1996, John Wiley & Sons, pp 513-514, "Schneier"). Applicants have carefully reviewed the cited references and respectfully assert that embodiments of the present invention as recited in Claim 2 are patentable over Spies in view of Deo and further in view of Schneier.

Applicants respectfully assert that Claim 2 overcomes the rejections of record as Spies teaches away from a combination with Deo, for the rationale previously presented, and respectfully solicit allowance of this Claim.

Applicants respectfully assert that Claim 2 overcomes the rejections of record by virtue of its dependency, and respectfully solicit allowance of these Claims.

Further with respect to Claim 2, Applicants respectfully assert that Spies

actually teaches away from embodiments of the present invention that recite

the limitation of "generating said public encryption key using the technique of

Diffie-Hellman Key Exchange" as recited by Claim 2.

In contrast, Spies teaches, "[t]he view computing unit 60 is not permitted,

however, to read the decryption capabilities" (column 9, lines25-26, emphasis

added) and "the individual packet keys are never made available to the viewer

computing unit..." (column 10, lines 46-47, emphasis added). Thus, in

accordance with the teaching of Spies, the recited "first logical unit" does not

decrypt the accessed encrypted signal, and further does not decrypt the accessed

encrypted signal using the recited "first decryption key."

Thus, Spies teaches away from key exchange, whether utilizing the

recited technique or not.

Doe fails to remedy this deficiency of Spies. Doe teaches "authentication"

of a smart card and an ATM based upon the well known technique of certificate

exchange. Accordingly, Doe depends upon a trusted third party, a "certifying

authority" (column 7, lines 45-60). Further, Doe teaches transfer of keys via

"certificates", e.g., "the smart card uses the terminal's public key that it received in the terminal's certificate" (column 7, lines 1-3).

By teaching trust in a third party "certifying authority" and by teaching transfer of keys via certificates, Doe actually <u>teaches</u> <u>away</u> from "generating said public encryption key using the technique of Diffie-Hellman Key Exchange" as recited by Claim 2.

For these further reasons, Applicants respectfully assert that Claim 2 overcomes the rejections of record, and respectfully solicit allowance of this Claim.

Claims 6 and 19 stand rejected as allegedly unpatentable over Spies et al. (US 6,055,314, "Spies") in view of Deo et al. (US 5,721,781, "Deo") and further in view of Yagawa (US 6,751,598, "Yagawa"). Applicants have carefully reviewed the cited references and respectfully assert that embodiments of the present invention as recited in Claims 6 and 19 are patentable over Spies in view of Deo and further in view of Yagawa.

Applicants respectfully assert that Claims 6 and 19 overcome the rejections of record as Spies <u>teaches</u> <u>away</u> from a combination with Deo, for the

rationale previously presented, and respectfully solicit allowance of these

Claims.

Applicants respectfully assert that Claims 6 and 19 overcome the

rejections of record by virtue of their dependency, and respectfully solicit

allowance of these Claims.

Further with respect to Claims 6 and 19, the rejection asserts that

Yagawa teaches "downloadable updates of the digital <u>content</u>" (emphasis

added). Applicants respectfully assert that one of ordinary skill in the art would

understand a fundamental difference between digital <u>content</u> and a computer

program for decrypting such digital content. For example, signal flow and

storage techniques are generally much different for the content as opposed to

programs. Applicants respectfully assert that a teaching of updateable digital

<u>content</u> fails to render obvious the limitation of replacing a decryption program

as recited by Claims 6 and 19.

For this further reason, Applicants respectfully assert that Claims 6 and

19 overcome the rejections of record, and respectfully solicit allowance of these

Claims.

In addition with respect to Claims 6 and 19, Yagawa teaches, an updating program "stored in the read only storage area" (column 2 lines 45-50). By teaching the updating program is stored in read only storage, Yagawa teaches that the updating program is itself not updatable. Consequently, Yagawa actually teaches away from embodiments in accordance with the present invention that recite replacing a decryption program as recited by Claims 6 and 19.

For this additional reason, Applicants respectfully assert that Claims 6 and 19 overcome the rejections of record, and respectfully solicit allowance of these Claims.

Applicants respectfully assert that Claims 6 and 19 overcome the rejections of record as Spies teaches away from claimed embodiments of the present invention as recited in Claims 6 and 19, for at least the rationale previously presented with respect to Claim 4, and respectfully solicit allowance of these Claims.

Still further with respect to Claim 6, Applicants respectfully assert that Spies in view of Deo and further in view of Yagawa fails to teach or fairly suggest the limitations of accessing and using a "second decryption key" as part of replacing a computer decryption program, as recited by Claim 6. Applicants

respectfully assert that Spies in view of Deo and further in view of Yagawa is silent as to use of the recited "second decryption key" in conjunction with replacing a computer decryption program, as recited by Claim 6.

For this still further reason, Applicants respectfully assert that Claim 6 overcomes the rejections of record, and respectfully solicit allowance of this Claim.

CONCLUSION

Claims 1-7 and 17-20 are pending in the present application. Applicants respectfully request reconsideration of the present application in view remarks presented herein.

The Examiner is invited to contact Applicants' undersigned representative if the Examiner believes such action would expedite resolution of the present Application.

Respectfully submitted,

WAGNER, MURABITO & HAO LLP

Date: _July 17, Zero 6_

Anthony C. Murabito
Reg. No. 35,295

Two North Market Street
Third Floor
San Jose, California 95113
(408) 938-9060